

الأمن السيبراني

Cyber Security






بسم الله الرحمن الرحيم



(وَلَقَدْ خَلَقْنَا الْإِنْسانَ وَنَعْلَمُ ما تُوَسْوِسُ بِهِ نَفْسُهُ وَنَحْنُ أَقْرَبُ إِلَيْهِ مِنْ حَبْلِ الْوَرِيدِ * إِذْ يَتَلَقَّى الْمُتَلَقِّيانِ عَنِ الْيَمِينِ وَعَنِ الشِّمالِ قَعِيدٌ * ما يَلْفِظُ مِنْ قَوْلٍ إِلاَّ لَدَيْهِ رَقِيبٌ عَتِيدٌ).

سورة ق



حقيبة
الأمن السيبرانـي
التوعوية

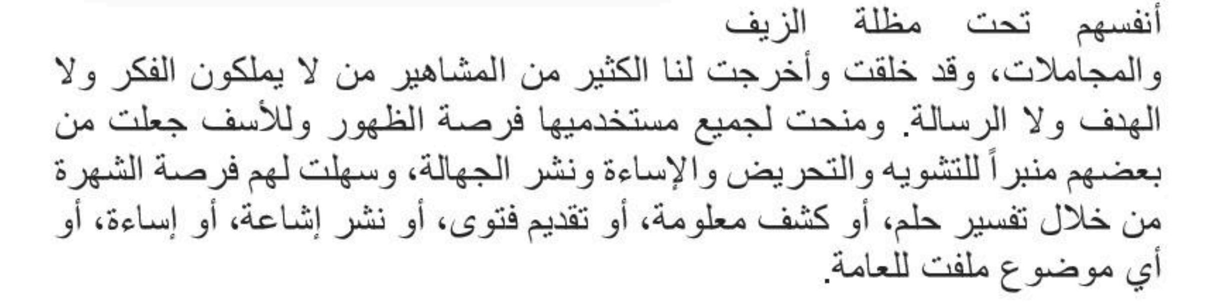
الفهرس

الفضاء السيبراني هو الفضاء الذي يعد عالماً إفتراضياً نعيشه بواقعنا الحاضر وجزء من حياتنا اليومية حيث يتيح لنا فرصة العمل والتعلم والتواصل والمشاركة لكثير من المعلومات مع الأصدقاء والغرباء في كثير من الأحيان. ومع الإنتشار السريع في التقنيات الحديثة وتوفر برامج التواصل الإجتماعي على المنصات المتعددة بين مختلف أنواع المستخدمين جعلت هذا الفضاء ساحة إلكترونية متاحة للصغير والكبير والمتعلم وغير المتعلم والسوي صاحب النوايا الحسنة وكذلك غير السوي ذو الطباع السيئة وظهرت لدينا عدة سلوكيات غير سليمة يصنف بعضها كجرائم معلوماتية، ومن هنا توجب علينا أن نتعلم كيف يكون التواجد الآمن في هذه البيئة الغير منتهية الأطراف والتي تجعل من العالم قرية صغيرة بين أيدينا نجوبها عبر أجهزة هواتفنا الذكية ونشارك بها بياناتنا ومعلوماتنا بشكل يؤثر على خصوصياتنا وسرية تعاملاتنا وبشكل قد يضعنا في فخ الخداع والتلاعب والسرقات الإلكترونية والاختراقات المؤذية والوقوع في المخالفات المعلوماتية والإلكترونية.



د. علي بن عيدروس بن علي البار
وكيل الكليات والمعاهد للتعليم الإلكتروني
الهيئة الملكية بينبع

اعتاد الناس التواصل في نطاق فيزيائي مكاني مرئي ومحدود، لنرى بعضنا البعض وجهاً لوجه ونتحاور وندردش ونتفاعل ضمن مساحات معروفة، ولكن مع تطور التقنيات والاتصالات نشأ لدينا ما يعرف بالفضاء السيبراني والذي قد غير من طريقة حياتنا وتعاملاتنا بشكل كبير وأصبحنا نتواصل مع بعضنا البعض في فضاء افتراضي واسع بلا حدود، نرى فيه الصديق والغريب والكبير والصغير والعاقل والجاهل وذوي النوايا الحسنة وغير الحسنة. فقد أثرت هذه البيئة على سلوك كثير من الناس وجعلت منهم أناس أقل تحفظاً ومنفلتين نحو استخدامات ومشاركات غير محدودة كسرت بها قيود الخصوصية والسرية في حياتنا. كما قد جعلت الكثير من رواد هذه البيئة يلبسون أقنعة متعددة ليخفون بها أنفسهم تحت مظلة الزيف والمجاملات، وقد خلقت وأخرجت لنا الكثير من المشاهير من لا يملكون الفكر ولا الهدف ولا الرسالة. ومنحت لجميع مستخدميها فرصة الظهور وللأسف جعلت من بعضهم منبراً للتشويه والتحريض والإساءة ونشر الجهالة، وسهلت لهم فرصة الشهرة من خلال تفسير حلم، أو كشف معلومة، أو تقديم فتوى، أو نشر إشاعة، أو إساءة، أو أي موضوع ملفت للعامة.



اليوم، يجب أن نعلم أن ساحات الاختلاط الأكبر ليست في الأسواق، أو الشوارع، أو النوادي كما يظن الكثير من الناس، بل أصبحت بداخل البيوت، من خلال استخدام الإنترنت وبرامج التواصل الاجتماعي والألعاب الإلكترونية وساحات الدردشة الإلكترونية وغيرها من التطبيقات. وقد يتسع الأمر ويكون الأثر أكبر عندما نتواجد في هذه البيئة من كل مكان وفي أي وقت وزمان وهو ما يحدث لنا في عصرنا الرقمي الحديث، فنحن نحمل بأيدينا أجهزة ذكية توفر لنا



خدمات الإنترنت اللاسلكية والتواصل المباشر والحي مع الناس عبر الهواتف النقالة والأجهزة المحمولة، ومن هنا يجب الاعتراف بأن تواجدنا في هذه البيئة السيبرانية ليس خياراً وإنما وسيلة ومطلب من متطلبات الحياة الحديثة.

من خلال هذه الحقيبة، سنتعرف على الكثير من المصطلحات الإلكترونية المتداولة في الفضاء السيبراني وكذلك المخاطر المحتملة من التواجد في هذه البيئة الافتراضية وكيف لهذه البيئة أثر على سلوكياتنا وأفعالنا وأقوالنا وحتى أخلاقنا عند التعامل مع الناس خلف أسوار الاتصالات الحديثة والتطبيقات المتعددة فنحن نعي أن ساحة الفضاء السيبراني لها الكثير من الفوائد، ولكن هناك الكثير من السلبيات والتي قد توصلنا إلى الجرائم المعلوماتية والإلكترونية. كما سنتعلم على وسائل الاستخدام والتعامل الآمن في هذه البيئة السيبرانية وطرق حماية الخصوصية وحماية المعلومات وحماية الفرد والعمل والمجتمع من العنف والاعتداء والاحتيال الإلكتروني بكافة أنواعهم وأشكالهم وطرقهم والتعرف على كيفية التصدي والإبلاغ عنهم ومنع حدوثهم.



المتدربين/ المتدربات الكرام:

أشكر لكم اختياركم حضور هذا البرنامج التدريبي والذي من خلاله نسعى إلى إكسابكم المهارات والمعارف المتعلقة بأمن المعلومات وأمن التواجد بالفضاء السيبراني سعياً إلى زيادة الوعي لديكم وجعلكم خط الدفاع الأول لمنع المخاطر والهجمات الإلكترونية المحتملة والبقاء في أمان بإذن الله، وحرصاً على تحقيق الهدف المرجو من التدريب فإننا نذكركم بما يلي:

1. التدريب الفعال هو الذي تشارك فيه جميع المتدربين بطرح الآراء والأفكار والمناقشة الهادفة.
2. العمل ضمن أفراد المجموعة في التمارين الجماعية يوسع دائرة الفائدة.
3. من حق أي متدرب أن يساهم بطرح فكرته أو رأيه.
4. الأفكار عزيزة عند أصحابها حرياً بنا أن ننصت لها.
5. أنماط التفكير تختلف من شخص لآخر.
6. الحضور في الوقت المحدد للبرنامج من عوامل النجاح.
7. التركيز على التدريب وتجنب المعوقات - كالجوال ونحوه - يوسع دائرة الاستفادة.
8. تقبل الدور الذي يسند إليك في المجموعة من عوامل نجاح إنجاز المهمة.
9. الخبرة في ذاتها وبذاتها ليس لها معنى إلا إذا استعملت.
10. ليس هناك فشل ولكن تجارب وخبرات وفرص للتعلم.
11. كم هو جميل أن نحرص على بناء علاقات طيبة مع المدرب والزملاء أثناء البرنامج التدريبي .
12. إن تحفيز أفراد مجموعتك في المشاركة في النشاطات يقوي فرص النجاح لديكم.
13. إن انتقال أثر التدريب وتطبيقه في البيئة العملية دليل نجاح.



اسم البرنامج:

حقيبة الأمن السيبراني التوعوية



الهدف العام للبرنامج:

توعية المتدربين بكيفية التواجد الآمن ضمن بيئة الفضاء السيبراني



وصف البرنامج التدريبي

برنامج تدريبي يهدف إلى مساعدة المستخدمين/ الموظفين على كيفية التعامل مع الانترنت من خلال ممارسة الأنشطة في البرنامج وتعزيز حماية وسرية وخصوصية البيانات الشخصية والعملية واتخاذ جميع التدابير اللازمة لتجنب المخاطر المحتملة في الفضاء السيبراني.

ماهي أهداف حقيبة الأمن السيبراني التوعوية؟

تتبلور أهمية الحقيبة التدريبية فيما يلي:

- التعريف بمصطلحات الفضاء السيبراني العامة والمعاني الخاصة
- توضيح أخطار الفضاء السيبراني ومنصات التواصل الاجتماعي
- بيان سبل تحقيق الأمن السيبراني الشامل
- ممارسة مبادئ وأساسيات الأمن السيبراني
- التعرف على الاستخدام الآمن والمشاركة الآمنة للمعلومات
- استشعار المخاطر التي تعصف بمنصات التواصل الاجتماعي
- توضيح أهمية القيم في تحقيق الفائدة من استخدام الفضاء السيبراني
- توضيح طرق مكافحة الجرائم المعلوماتية بالمملكة العربية السعودية









الفئة المستهدفة:

منسوبي الهيئة الملكية للجبيل وينبع



مدة البرنامج:

يوم واحد (5 ساعات تدريبية)

الوسائل المقترحة:

عروض تقديمية – ورش عمل – نشاطات – جلسات نقاش وحوار.





التقويم الذاتي القبلي.

يمكن الوصول عبر مسح الكود الظاهر.





تقويم البرنامج التدريبي

(استمارة تقويم البرنامج من حيث الأهداف، المحتوى، الأساليب، المدرب، بيئة التدريب، الوقت) يمكن الوصول عبر مسح الكود الظاهر.

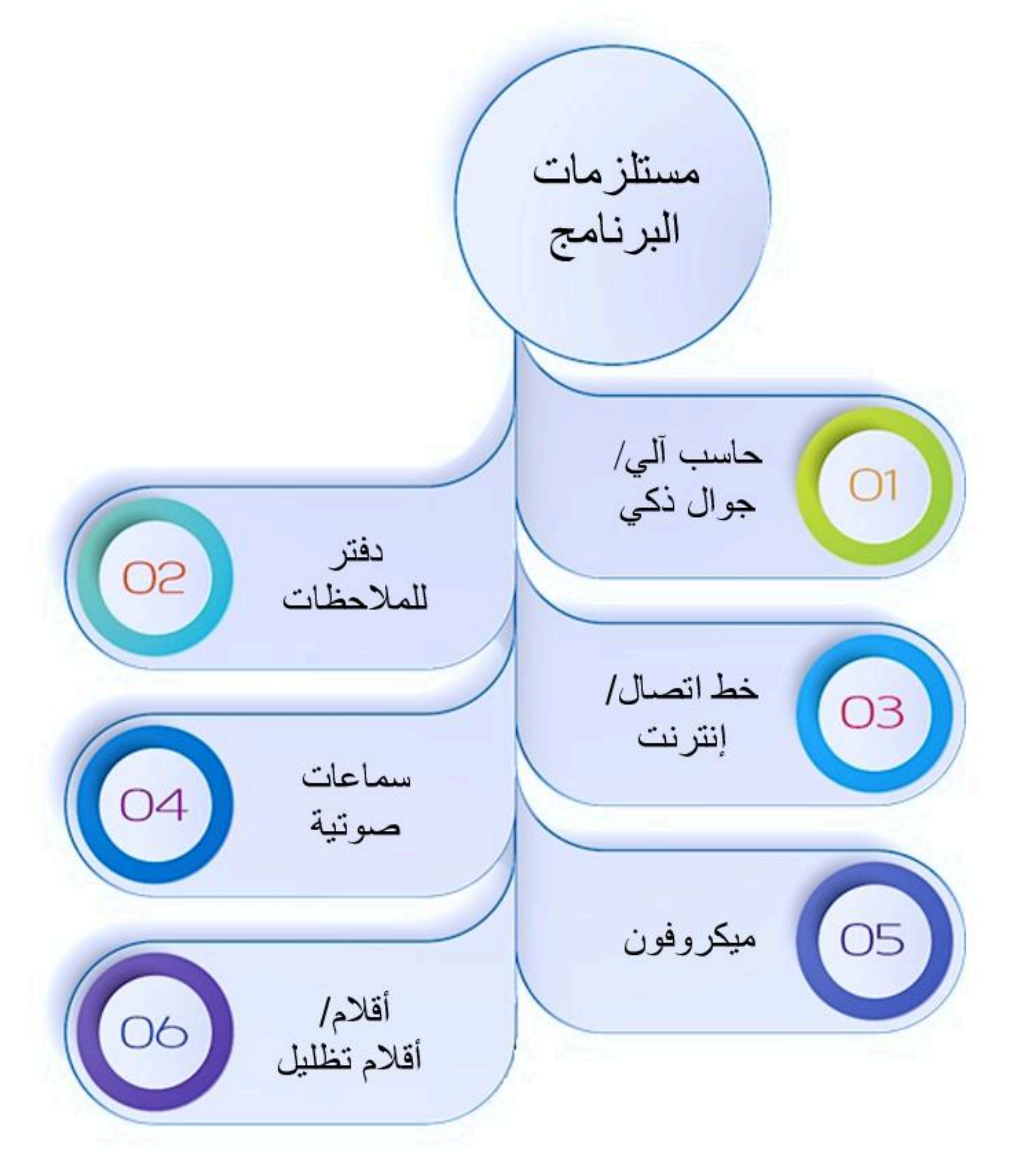




التقويم الذاتي البعدي.

يمكن الوصول عبر مسح الكود الظاهر.




مستلزمات
البرنامج
01
حاسب آلي/
جوال ذكي
02
دفتر
للملاحظات
03
خط اتصال/
إنترنت
04
سماعات
صوتية
05
ميكروفون
06
أقلام/
أقلام تظليل


الأهداف
الزمن
الإجراءات
النقاش

اليوم التدريبي	الجلسة	عنوان الجلسة	الزمن
١		الافتتاح ومقدمة البرنامج	مقدمة ٢٠ دقيقة
		حقائق وأرقام إحصائيــة إلكترونيــة	إحصاءات ٢٥ دقيقة
	الجلسة الاولى	الفضاء السيبراني	الجلسة ١ ٣٠ دقيقة
	النشاط الاول	الحقائق والاعتقادات الخاطئة	نشاط ١ ٢٠ دقيقة
		استراحة	استراحة: ٢٠ دقيقة
	الجلسة الثانية	أخطار التواجد بالفضاء السيبراني وأثره على سلوكيات المستخدم	جلسة ٢: ٢٥ دقيقة
	الجلسة الثالثة	الحماية بالفضاء السيبراني	جلسة٣: ٢٠ دقيقة
	النشاط الثاني	جرة الاعتراف	نشاط ٢: ٢٥ دقيقة
		استراحة	استراحة: ٢٥ دقيقة
	الجلسة الرابعة	حماية المعلومات والخصوصية بالفضاء السيبراني	جلسة ٤: ٢٠ دقيقة
	النشاط الثالث	الهندسة الاجتماعية	نشاط ٣: ٢٠ دقيقة
	الجلسة الخامسة	إرشادات تطبيق التواجد الأمن بالفضاء السيبراني	جلسة ٥: ٢٠ دقيقة
	النشاط الرابع	مقياس الممارسات الإلكترونية الخاطئة	نشاط ٤: ١٥ دقيقة
	خاتمة	الوصايا العشر في الأمن السيبراني	خاتمة: ١٠ دقيقة
	استبانة	استبانة تقييم البرنامج التدريبي	استبانة: ٥ دقائق

الجدول الذاتي في الملحق (أ) يساعد على أن تتأملوا فيما تعرفون حول موضوع التدريب، وما تريدون معرفته، وما ستتعلمون خلال هذا التدريب بعد كل جلسة ونشاط تدريبي.

1- في بداية التدريب سجل في العمود الأول ما تعرف عن موضوع التدريب (Know)، وفي العمود الثاني سجل ما تريد أن تعرف (Want to Know).

2- خلال التدريب اكتب في العمود الثالث ما تعلمته (Learned).

3- في حالة وجود أسئلة لديك خطرت في بالك ولم تجد الإجابة عليها أثناء التدريب، فاكتب أسفل الجدول (Question) حتى تبحث عن إجاباتها أو تقوم بطرحها على المدرب خلال البرنامج التدريبي.

K ماذا أعرف؟	W ماذا أريد أن أعرف؟	L ماذا تعلمت؟

أسئلة لازالت لديّ (Q) ؟

....

....

....

....

....

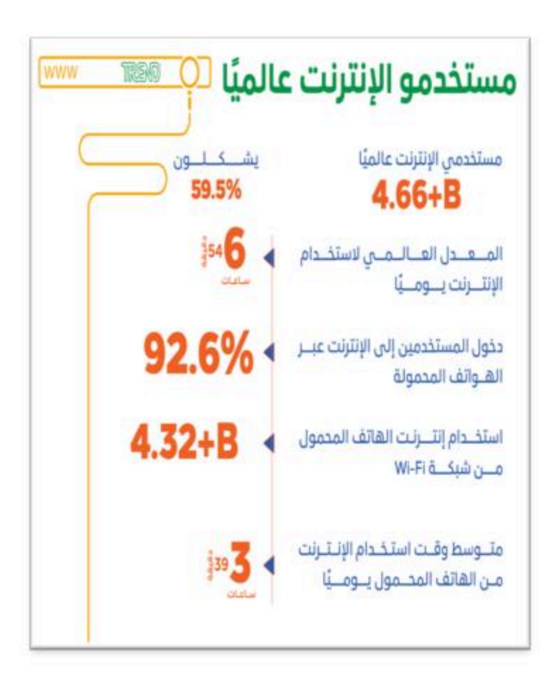
....

استبانة التقييم القبلي لقياس وعي المستخدمين بمفاهيم الأمن السيبراني.

أرجوا قراءة العبارات التالية والإجابة بـ (نعم) حال الموافقة على ما تم ذكره بالعبارة والاجابة بـ (لا) حال عدم الموافقة عليها:

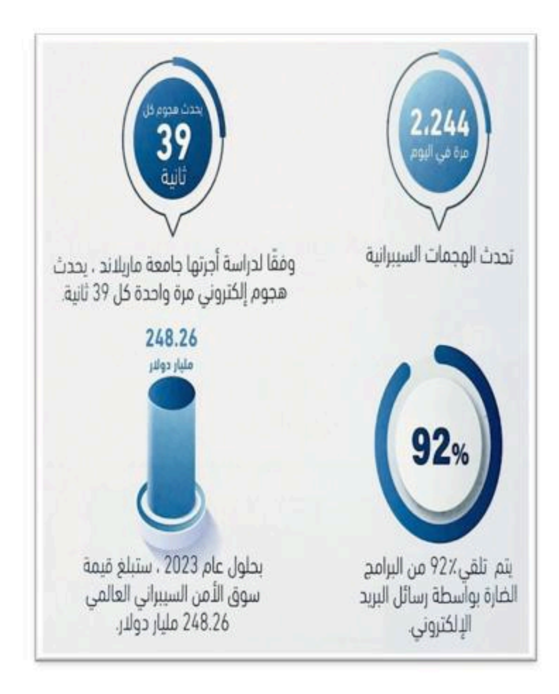
العبـــــــــــــــارة	نعم	لا
أقوم باستخدام برمجيات وتطبيقات خاصة لحماية جهازي من الاختراق والتجسس والفيروسات		
احتفظ بالبيانات الخاصة بي في أكثر من مكان لتفادي فقدانها او تلفها		
أقوم بنسخ البيانات الخاصة بي احتياطياً في ذاكرة خارجية وحفظها بمكان آمن		
اسمح بمشاركة معلوماتي الشخصية للأصدقاء عبر الإنترنت وبرامج التواصل الاجتماعي وغيرها من الوسائل بالفضاء السيبراني		
اسمح بمشاركة معلوماتي الشخصية للغرباء عبر الإنترنت وبرامج التواصل الاجتماعي وغيرها من الوسائل بالفضاء السيبراني		
اسمح بمشاركة بعض معلوماتي الشخصية غير الحساسة للأصدقاء عبر الإنترنت وبرامج التواصل الاجتماعي وغيرها من الوسائل بالفضاء السيبراني		
اسمح بمشاركة بعض معلوماتي الشخصية غير الحساسة للغرباء عبر الإنترنت وبرامج التواصل الاجتماعي وغيرها من الوسائل بالفضاء السيبراني		
احرص على تجنب مشاركة المعلومات المخالفة للعقيدة، او الدين، او القوانين، او الأعراف، او التقاليد		
دائما ما اراعي أراء الآخرين ومشاعرهم عند مناقشة موضوع ما عبر الإنترنت		
لدي وعي كافي بأنظمة المملكة العربية السعودية المتعلقة بالأمن السيبراني يمكنني من التعامل مع الإنترنت وبرامج التواصل الاجتماعي بشكل آمن وصحيح		
أشدد على ضرورة توعية المستخدمين/ الموظفين/ الطلبة بمفاهيم الامن السيبراني والتعليمات والقوانين والمخالفات والعقوبات المتعلقة باستخدام الإنترنت وبرامج التواصل الاجتماعي		
أؤيد وضع إجراءات وسياسات واضحة لحفظ الأمن السيبراني الخاصة بمشاركة المعلومات ونقلها عبر الإنترنت		




مستخدمو الإنترنت عالميًا
www
مستخدمي الإنترنت عالميًا
4.66+B
يشـكـلـون
59.5%
المـعـدل العـالـمـي لاستخـدام الإنتـرنت يـومـيًا
6 ساعات 54
دخول المستخدمين إلى الإنترنت عبـر الهـواتف المحمولة
92.6%
استخـدام إنتـرنت الهاتف المحمول مـن شبكـة Wi-Fi
4.32+B
متـوسط وقـت استخـدام الإنـتـرنت مـن الهاتف المحـمول يـومـيًا
3 ساعات 39


+41M
عدد اشتراكـات الهاتف المتنقل
123.63
معدل الاشتراك\100 فرد
33.58M
مستخدمو الإنترنت (على كافة الأجهزة)
95.7%
مستخدمي الإنترنت من إجمالي السكان
TREND
7 ساعات و45 دقيقة
متـوسط وقـت الاستـخـدام


مستخدمي منصات التواصل الاجتماعي
13.00M
76.9% 23.1%
27.80M
59.5% 40.5%
15.00M
55.6% 44.4%
9.20M
76.9% 23.1%
5.00M
78.9% 21.1%
19.60M
48.1% 49.6%
12.45M
93.6% 6.4%


2,244
مرة في اليوم
تحدث الهجمات السيبرانية
يحدث هجوم كل
39
ثانية
وفقًا لدراسة أجرتها جامعة ماريلاند ، يحدث هجوم إلكتروني مرة واحدة كل 39 ثانية
92%
يتم تلقي 92٪ من البرامج الضارة بواسطة رسائل البريد الإلكتروني
248.26
مليار دولار
بحلول عام 2023 ، ستبلغ قيمة سوق الأمن السيبراني العالمي 248.26 مليار دولار




وقت متابعة الإنترنت والوسائط المتعددة يوميًا
7 ساعات و45 دقيقة
مشاهدة مقاطع الفيديو
4 ساعات و13 دقيقة
مشاهدة التليفزيون عبر الشبكات أو الإنترنت
3 ساعات و6 دقائق
شبكات التواصل الاجتماعي
2 ساعتان و42 دقيقة
قراءة الصحف (الورقية أو على الإنترنت)
1 ساعة و45 دقيقة
الاستماع لخدمات البث الموسيقي
49 دقيقة
الاستماع لشبكات الراديو
1 ساعة و17 دقيقة
الاستماع للبودكاست
1 ساعة و58 دقيقة
ألعاب الفيديو


الأجهزة المستخدمة للوصول إلى الإنترنت
نسبة إلى عدد مستخدميه
99.57%
الهاتف المتنقل
26.65%
الحاسب المحمول
9.64%
الحاسب المكتبي
4.47%
الحاسب اللوحي Tap
0.42%
أجهزة أخرى


عدد مرات استخدام الإنترنت
94%
مرة واحدة على الأقل يوميًا
4%
مرة واحدة على الأقل أسبوعيًا
0.23%
مرة واحدة على الأقل شهريًا
0.06%
مرة واحدة في الأشهر الثلاث الأخيرة
اللغة المستخدمة في تصفح الإنترنت
82%
العربية
24%
الإنجليزية
13%
أخرى


سلوك البحث على الإنترنت
98.9%
استخدموا محرك بحث تقليدي في الشهر الماضي
45.3%
استخدموا بحث صوتي أو أوامر صوتية
Search...
60.0%
استخدموا مواقع التواصل الاجتماعي كمصدر للبحث
31.7%
استخدموا أدوات التعرف على الصور للبحث


أعلى التطبيقات تحميلاً
TIKTOK
WHATSAPP
SNAPCHAT
LIKEE
IMO
TELEGRAM
MICROSOFT
ZOOM
INSTAGRAM
FACEBOOK


أكثر المواقع تصفحًا
semrush
293M
Google.com
109M
youtube.com
58.1M
Twitter.com
51.7M
Google.com.sa
48.5M
Sabq.org
46.8M
Wikipedia.org
41.5M حراج
Haraj.com.sa
41.4M
Madrasati.sa
38.5M
Facebook.com



















المصدر: TREND | Digital Communication

يمكن الوصول للتقرير من خلال الرابط: https://trenddc.com/report/saudi-digitization2021/



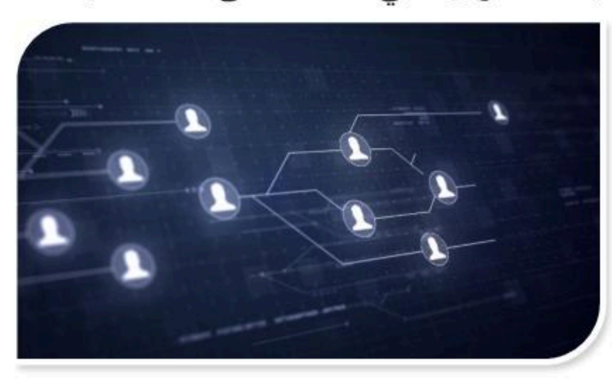
الجلسة الأولى

ماذا نقصد بالفضاء السيبراني Cyber-sphere؟

كلمة فضاء (Sphere) تعني الساحة والتي يمكن أن تكون مساحة للتواجد فيما بيننا وعند إضافة كلمة سيبر (Cyber) فتصبح ساحة الإنترنت او الوصلة الرقمية التي تضيف خاصية تكنولوجيا المعلومات وبها تكسر قيود الزمان وحدود المكان فتعطي إمكانية التواصل الإلكتروني على شبكات الإنترنت، وتجمع الأصدقاء مع الأصدقاء وقد يكون مع الغرباء، والتواصل في هذه الساحة الافتراضية على هيئة تبادل وتشارك أنواع مختلفة من الرسائل بين المستخدمين ومنها على سبيل المثال تبادل الرسائل النصية والصوتية والرسومية الثابتة والمتحركة والفيديوهات وغيرها من الوسائط المتعددة.

إذاً هل الفضاء السيبراني حقيقة؟

الجواب المؤكد هو أنه حقيقة ضمن ساحة افتراضية غير ملموسة وهي ليست ساحة محدودة التفاعل مثل بعض الأشياء الأخرى التي أعتدنا على استخدامها مثل مشاهدة التلفزيون، أو إجراء مكالمة هاتفية، أو الاستماع إلى الراديو، بل أصبحت بيئة ينغمس فيها الشخص ذهنياً إلى درجة كبيرة فتستحوذ عليه بطريقة فريدة وتجذبه إليها حيث ينسى واقعه الذي يعيشه. كما أن هذا الفضاء مليء بأسماء الأماكن وشبكات التواصل الاجتماعي والمنتديات والمواقع الإلكترونية والألعاب الإلكترونية وغير ذلك وحين نتواجد هناك ننضم الى مجموعات كبيرة من الاشخاص من قد تربطنا بهم علاقة أوقد لا نعرفهم أصلاً، وهذا ما يجعل من هذه البيئة فريدة من نوعها لتكسر كثير من الحواجز.





هل هناك آثار إيجابية أو سلبية من تواجدنا في الفضاء السيبراني؟

قد نعلم أن هنالك فوائد كثيرة من التواجد في الفضاء السيبراني فقد وجدنا أنفسنا أمام خيارات متعددة ومفيدة خلال جائحة فيروس كورونا المستجد كوفيد-19 فعلى سبيل المثال كان هنالك خيارات العمل عن بعد وعقد الاجتماعات الافتراضية وكذلك التوجه إلى التعليم عن بعد من خلال المنصات المختلفة وإتاحة حضور الفصول الافتراضية واستكمال عملية التعليم والتعلم دون توقف وقد زادت هذه الحلول من زيادة الأمان الصحي والرعاية المجتمعية والاتزان الاقتصادي وغيرها من الفوائد ولكن في الوقت ذاته ظهرت لدينا الكثير من المخاوف والإشكالات وذلك بسبب إما قلة الوعي باستخدام الأدوات التقنية والتعامل معها ومعرفة الاستخدام الصحيح لها وطرق حفظ الخصوصية ومشاركة المعلومات أو لأسباب عدم فهمنا الواسع للبيئة السيبرانية وإدراك مخاطرها المحتملة وما يترتب على ذلك من عقوبات وغرامات وغيرها من الأمور الخطيرة.



من هنا يجب أن نعي أن هناك أثار سلبية من التواجد في هذه الساحة الافتراضية وهنالك فرص للتعرف والالتحاق بشبكات واسعة من الأشخاص وكم كبير من الاتصالات التي تقتحم حياتنا وخصوصياتنا في كل وقت وحين، وكيف من الممكن أن يتغير سلوكنا عندما ندخل في هذه الساحة الافتراضي، فقد تخذلنا الغرائز ويتغير سلوكنا عما كنا عليه في الواقع الحقيقي مع الناس وجهاً لوجه، وقد نجد أنفسنا لنتعامل مع أشخاص مختلفين عنا اجتماعياً وثقافياً ودينياً وسلوكياً، فهي ساحة تخدم روادها إن أحسنوا استعمالها ولها جانب مظلم يجب أن نحذر منه خصوصاً عندما نواجه بعض ضعفاء النفوس وغير الأسوياء والشواذ والمجرمين والغامضين والحاقدين والشرسين وللأسف فهم يجدونها ساحة جاذبة لهم ليختفوا خلفها بحجة اللهو واللعب والدردشة ويستغلوا ضحاياهم ويتعاملوا معهم وكأن الأشياء الغير مقبولة في الواقع الحقيقي مقبولة والأفعال الغير مسموحة مسموحة وهو الأمر الذي يشكل الخطر الكبير في هذه الساحة الإلكترونية لنرى الكثير من السلوكيات الغير سوية مثل التنمر الإلكتروني والتسلط والإيذاء والترهيب والابتزاز والكراهية والعدوانية وفي نهاية المطاف إلى ما يفضي إلى الجريمة الإلكترونية والمعلوماتية.





فماذا نقصد بالتنمر والتسلط والإيذاء الإلكتروني Cyberbullying ؟

لا نعني بالتنمر أن يكون الشخص نمراً، وإنما أن يصبح سلوكه عدائياً شرساً فظاً ذو أخلاق سيئة، فيختار المعتدي من هو أضعف منه جسدياً أو نفسياً أو أعلى مكانةً وسلطة وقوة لكي يؤذيه بطرق متعددة. فهو سلوك عدائي متعمد ويحدث بشكل مكرر من جانب شخص واحد أو مجموعة من الأشخاص غرضهم إيذاء الآخرين من خلال استخدام الوسائل الإلكترونية في الفضاء السيبراني وهم في حالة وعي تام. وتتمثل هذه السلوكيات في إلصاق التسميات غير اللائقة، إرسال الرسائل المهينة والغير مرغوب فيها، نشر الإشاعات والمعلومات المغلوطة عن الضحايا، ونشر الصور ومقاطع الفيديو المحرجة، والتي غالباً ما تسبب الشعور بعدم الارتياح والحرج الشديد والألم النفسي والمعنوي للضحية.

وماذا نقصد بالترهيب والتخويف والتتبع الإلكتروني Cyberstalking ؟



الترهيب الإلكتروني عبارة عن مجموعة من الأفعال والسلوكيات على الإنترنت وتحدث في ساحات الفضاء السيبراني موجهة إلى شخص معين تصيبه بالقلق والشعور بالخوف وعدم الراحة. ومن الأمثلة إرسال رسائل عدوانية غرضها الابتزاز أو التخويف والترهيب ونشر معلومات كاذبة وشائعات سيئة وافتراءات قد تدمر الوضع الاجتماعي للضحية، وكذلك تتبع الضحية لجمع معلومات قد تؤثر على علاقاته الشخصية والعائلية والمهنية الحالية والمستقبلية وقد ترتبط بأنواع مختلفة من الابتزاز وطلبات افعال أمور محددة والامتناع عنها وقد يرتبط ذلك بمطالبات مالية ومادية.



وماذا نقصد بالممارسات الإلكترونية الخاطئة؟

الممارسات الإلكترونية الخاطئة تتمثل في الاستخدام غير الآمن لبرامج التواصل الاجتماعي (فيسبوك، تويتر، سناب شات، إنستقرام، تيك توك، وغيرها) وتبادل المعلومات الشخصية والمعلومات الحساسة والسرية عبر هذه التطبيقات بشكل غير آمن. كما أن حساسية المعلومات تعتمد على مدى أهمية وسرية المعلومات المتبادلة فقد يكون نشر الصور الشخصية ومقاطع الفيديو الخاصة وما تحتويه من قضايا أسرية واجتماعية وصحية وخطط مستقبلية وأسرار شخصية، أو عائلية، أو مهنية، أو مالية نوع من الممارسات الخاطئة. إضافة إلى ذلك تجاهل الإعدادات الصحيحة لحماية الخصوصية ضمن هذه التطبيقات وإتاحة المعلومات للعوام، وأيضاً استخدام هذه البرامج في نشر المعلومات الغير صحيحة والشائعات من دون التأكد من مصدرها وتجاهل السياسات والقوانين والأنظمة والعقوبات المترتبة.



إحصائيات عامة عن العدوانية الإلكترونية

01
18% من الأطفال والمراهقين والشباب حول العالم تعرضوا للعدوانية الإلكترونية

02
18% من الذين تعرضوا للعداء الإلكتروني قد أثر ذلك سلباً على مستواهم الدراسي والعملي وسبب لهم الخوف وعدم الأمان

03
7 من كل 10 مستخدمين للانترنت في العالم تعرضوا للإساءة في مرحلة معينة من حياتهم

04
79% من الآباء ذكروا أن أطفالهم تعرضوا للتهديد وبإيذاء جسدي أثناء اللعب على الانترنت

المصدر: مبادرة العطاء الرقمي
يمكن الوصول للمصدر من خلال الرابط: https://cyberbullying.attaa.sa



يتم توضيح الحقائق وتصحيح الاعتقادات الخاطئة الأكثر شيوعاً في الفضاء السيبراني من خلال شرح ١٦ عبارة يعتقد بصحتها.



يقوم المتدرب بقراءة العبارات، ويقوم بوضع العلامة (√) إذا كانت العبارة صحيحة وتحاكي الواقع أو العلامة (X) إذا كانت تمثل مفهوم سائد واعتقاد خاطئ.



بعد ذلك يقوم المدرب بشرح كل عبارة وتوضيح لماذا هي حقيقة أو مفهوم خاطئ وتبيان أثار هذا الاعتقاد على سلوكيات الناس ومدى المخاطر المحتملة من ذلك في الفضاء السيبراني.

يمكن الوصول للنشاط من خلال الرابط:

https://fs7.formsite.com/alibaro/j5gucn8w7l/index.html



العبارات	صح	خطأ
بشكل عام، العدوانية جزء طبيعي من نمو الفرد متطلب لبناء الشخصية وينتهي دون تدخل		
معظم حالات العدوانية السيبرانية تكون لفظية ومن مصدر خارجي لا يستدعي القلق		
في كثير من الأحيان يولد الإنسان بطبيعته متنمراً او عدائياً متحيزاً		
المتنمرون يتخلصون من سلوكياتهم العدوانية باستخدام التقنية ودون قصد الإيذاء		
المتنمرون هم ذوي مهارات اجتماعية ممتازة ولديهم صداقات وثقة عالية بأنفسهم		
عادة ما يكون هناك آخرون يشهدون وقوع حالات التنمر والعدوانية		
المتنمرون يعانون من تدني احترم الذات ويتم رفضهم من قبل اقرانهم او المجتمع		
يجب أن يكون هنالك شخصية الضحيـة لتتم حالة التنمر والعدوانية		
ضحايا التنمر يجب عليهم الوقوف بشدة ومهاجمة المتنمرين بالمثل		
وضع القوانين يساهم في الكشف والحد من حالات العدوانية السيبرانية		
الاعدادات التقنية ستحمي المستخدمين من حالات العدوانية السيبرانية		
مسؤولي تقنية المعلومات عليهم مسؤولية حماية المستخدمين ومنع العدوانية السيبرانية		
لم اتعرض للعدوانية السيبرانية فاعتقد بعدم وجودها ولا تستحق الاهتمام		
العدوانية السيبرانية لن تتحول الى عدوانية جسدية طالما هي عبر الانترنت		
العدوانية السيبرانية لن تشكل أخطار على اختراق الأجهزة او المعلومات او الخصوصية		
العدوانية السيبرانية لا تصل إلى حد تصنيفها من ضمن الجرائم المعلوماتية		



الجلسة الثانية

ما هي الجرائم الإلكترونية والمعلوماتية Cybercrimes ؟

هي المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء الضحايا أو تحقيق أذى مادي أو نفسي لهم، إما بشكل مباشر أو غير مباشر وذلك باستخدام شبكات الاتصالات والإنترنت وعبر منصات وبرامج التواصل الاجتماعي وغرف الدردشة ضمن الألعاب والبريد الإلكتروني وعبر تطبيقات الهواتف الذكية والأجهزة اللوحية وما شابهها، وفيما يلي بعض الأمثلة لتلك الجرائم:



1. الاستهزاء والتشهير بالآخرين وتشويه السمعة وإلحاق الضرر بالضحايا
2. الاختراق وسرقة المعلومات وتزيفها والإتجار بها
3. سرقة الحسابات وانتهاك الخصوصية وانتحال الشخصية
4. الترهيب والتهديد والابتزاز؛ وحمل الضحايا على القيام بفعل عمل ما أو الامتناع عنه
5. التنمر والتسلط والأذية ونشر الكراهية والعنف بين أفراد المجتمع
6. التحرش والمضايقة لكافة فئات المجتمع من الجنسين و شتى الأعمار
7. جمع ونشر الصور والمقاطع الإباحية الهادمة للقيم الدينية والآداب العامة في المجتمع
8. هدم القيم الأسرية والمواطنة ونشر العنصرية بين أفراد المجتمع

وليس من المستغرب وجود هذا الكم الكبير من المخالفات في هذا الفضاء الافتراضي الواسع وما قد يحدث به في الحقيقة هو ليس من الأمور الاعتيادية كما يعتقد البعض بل هي ممارسات مصنفة بأن تكون من الجرائم استنادا على نظام مكافحة جرائم المعلوماتية بالمملكة العربية السعودية والذي تم إقراره في مجلس الوزراء السعودي رقم 79 وتاريخ 1428/3/7 هـ، وتمت المصادقة عليه بموجب المرسوم الملكي الكريم رقم 17 /م وبتاريخ 1428/3/8 هـ، والذي يهدف إلى الحد من وقوع الجرائم الإلكترونية والمعلوماتية وقد سنت به العقوبات الصارمة والتي قد تصل إلى السجن لمدة ١٠ سنوات في أقصاها وغرامات مالية قد تصل إلى ٥ ملايين ريال في حدها الأعلى. للاطلاع وتفاصيل أكثر عن النظام يرجى نسخ الكود الظاهر.



ماذا بعد ذلك؟ هل التواجد في الفضاء السيبراني يعتبر آمنـاً؟



لعله من أحد أهم الأسئلة التي تدور بالأذهان، ولكن يجب أن نعي أن الفضاء السيبراني ساحة جامعة لمختلف النوعيات من البشر ونعلم أن الأطفال والشباب هم أكثر عرضة لمخاطر الفضاء السيبراني ومن الطبيعي أن يشعروا بالفضول وقد يريدون استكشاف كل جديد وفي الواقع هم لا تنقصهم الخبرة في استخدام التطبيقات المختلفة، بل قد يفوقون الكبار براعة في استخدامها، ولكن ليس لديهم النضج الكافي لإدراك المخاطر المحتملة ونتائج التعامل والتواصل المفتوح في هذه البيئة الافتراضية. الساحة السيبرانية تتضمن الاحتكاك ببعض الغرباء والناس الخطيرين، وهؤلاء كثيراً ما لا يخضعون للمراقبة فهم في ساحة يعلمون أن الأطفال أحد ضحاياها ويتعرضون فيها للمخاطر والإهمال في الوقت ذاته.

ويعتبر ذلك من أخطر سلبيات التعامل في هذه البيئة المفتوحة والتي بدورها تغير من سلوكيات الناس ومشاعرهم وقيمهم وإخفاء هويتهم الحقيقية، وكيف يستغل المجرمون تلك التغيرات فلربما نعلم بعض الأشياء عن انتحال الهوية، التلصص، التحرش، السرقات للحسابات وبذلك نضع كلمات سر خاصة وقوية لضمان الأمان قدر الإمكان ولكن لربما لا ندرك كيف أننا نسهم من خلال بعض الممارسات الخاطئة في احتمال تعرضنا المباشر للخطر لكي نقع في فخ التنمر أو الترهيب أو الابتزاز ... فعلى سبيل المثال عندما نجلس في غرفة النوم ونحن نخبر العالم كله في فيسبوك، تويتر، سناب شات، إنستقرام وغيرها من التطبيقات بكل شيء فعلناه في ذلك اليوم ونشاركهم الصور والمقاطع الطريفة لمناسباتنا ومقابلاتنا العائلية وحتى الوجبات الشهية وغيرها من الأحداث الخاصة، بينما عندما نكون في السوبرماركت مثلاً، فلن نخبر أي غريب أو مجهول نراه وجهاً لوجه عن تلك الأشياء.

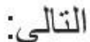


والسؤال الذي يطرح نفسه لماذا يحدث هذا لنا في هذه الساحة السيبرانية؟

الجواب المثير للاهتمام هو أننا في الحقيقة ننسى أنفسنا في لحظات وربما نطلع ملايين الغرباء على خصوصياتنا بسبب تأثيرات عدم الإحساس بالتحفظ في الفضاء السيبراني. من هنا يجب علينا التفكير بما سنشاركه مع الناس في هذا الفضاء السيبراني، فأنت تملك المعلومة وهي خاصة بك حتى تقوم بالنقر على زر إرسال أو مشاركة، عندها ستكون ملك للغير وليست من ممتلكاتك الشخصية كما كانت. كما أن هنالك دور كبير على الآباء والأمهات وكل رب أسرة وكل راع فهم شركاء أساسيين في حماية أبنائهم وذويهم على الإنترنت. ويجب أن يكون دخول كل ابن وابنة لساحة الفضاء السيبراني ضمن حدود وصلاحيات ورقابة عالية من الوالدين فقد يتعرضون للكثير من المضايقات وهم يمارسون الألعاب الإلكترونية من خلال الدردشة أو عند استخدام برامج التواصل الاجتماعي ومشاركة المعلومات وهي في الحقيقة قد تكون جرائم في حقهم مؤثرة بشكل سلبي على حياتهم الأسرية والاجتماعية والعلمية وغيرها من الجوانب والتي قد تسبب الضرر النفسي والجسدي إن لم يحسن التصرف وأخذ التدابير الصحيحة ومعالجتها ومنعها منذ بداياتها.

ما هو العمر المناسب للتواجد بالفضاء السيبراني واستخدام برامج التواصل الاجتماعي والالعاب الإلكترونية؟

معظم التطبيقات والالعاب تم تصنيفها بناء على المحتوى الذي يمكن مشاهدته من خلالها ولذلك تم تصنيف البرامج الاكثر انتشارا واستخداما حسب التصنيف العمري التالي:





تويتر

+17

يوتيوب

+17



انستقرام

+12



فيس بوك

+12



تيك توك

+12



سناب شات

+12



الجلسة الثالثة

ماذا نعني بالأمن السيبراني؟

"هو مجموعة من التقنيات التي تقوم بحماية وسلامة الأجهزة والشبكات والبرامج والبيانات من الهجوم والتلف أو الوصول غير المصرح به، ويمتد إلى أنه مجموعة من الأدوات والسياسات والمفاهيم الأمنية، وضمانات الأمان والمبادئ التوجيهية التي تسير على نهج إدارة المخاطر والإجراءات، وتعد أفضل الممارسات والضمانات التقنية التي تستخدم لحماية أصول المنظمة والمستخدم" (المبيض، ٢٠٢٠، ص.١٣).



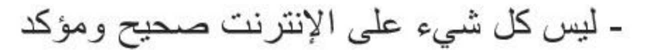
كيف أحمي نفسي سيبرانياً؟



الجواب لهذا السؤال يعتبر خارطة الطريق ودليل لبر الأمان عندما نتواجد في ساحة الفضاء السيبراني. ولعل أبسط إجابة لهذا السؤال هو أن نزيد من وعينا ونقوم بزيادة إدراكنا بالأدوات والسياسات والمفاهيم الأمنية المتعلقة بالأمن السيبراني لنعي المخاطر المحتملة ونفهم طبيعة التعامل في هذه البيئة المفتوحة مع مختلف الأنواع من البشر، وعلينا أن نجعل بقائنا في الفضاء السيبراني ضمن حدود الأمن والأمان.

وفيما يلي سنتطرق إلى عدة محاور ونصائح مهمة تزيد من الوعي المعرفي لدينا. ففي الفضاء السيبراني، ليس كل ما نراه هو حقيقة، فهناك الكثير من المواد التي قد تكون شائعات أو معلومات مغلوطة وبها تزييف للحقائق ويجب أن نعلم ما يلي:





- ليس كل شيء على الإنترنت صحيح ومؤكد
- من نقابلهم على الإنترنت قد يخفون هويتهم ويتعاملون معنا بزيف
- الصور والمقاطع قد تظهر لنا معنى مختلف عن الحقيقة
- كل ما تم وضعه على الإنترنت أصبح ليس ملك لصاحبه وخاصته



- الخصوصية على الإنترنت أكثر عرضة للكشف فلا مجال للأسرار

مراقبة السلوكيات ضمن البيئة السيبرانية



يجب علينا أن نعلم بأن تأثير البيئة السيبرانية كبير علينا فعندما نتحدث إلى الأشخاص عبر الإنترنت فنحن لا نرى تعابير الوجه ولا لغة الجسد ولا الإشارة وهذا قد يعطينا حرية أكبر لقول أي شيء وفعل أي شيء عكس ما إذا كنا نقابلهم وجهاً لوجه. وكذلك يجب أن نعلم أن من نتعامل معهم في البيئة السيبرانية فهم الأشخاص ذاتهم ولديهم نفس المشاعر والأحاسيس ولا يعني أن تواجدهم خلف الشاشات بأسماء مستعارة وبصور شخصيات كرتونية بأنهم أشخاص مختلفين لا يتأثرون بما نقول أو نفعل أو نشارك.



العواقب المحتملة من تعاملاتنا في الفضاء السيبراني

كل ما نقوم بكتابته أو فعله ضمن الساحة السيبرانية سنتحمل نتيجته. وعليه يجب أن نفكر قبل القيام بأي شيء فما نقوم به سوف يظهر للجميع دون حدود وقد يصل للملايين خلال ساعات. فاحرص على ما يلي:

* لا تشارك معلوماتك الشخصية والحساسة مثل أرقام الهوية، أرقام الهاتف، عنوان المنزل، معلومات العائلة المالية والخطط المستقبلية وغيرها.

* لا تشارك ما يزعج الآخرين ويؤذيهم من معلومات، وصور، ومقاطع فيديو، وغيرها.

* لا تشارك محتويات مخالفة للآداب والقيم والأعراف.

* لا تشارك ما يثير الفتن والعنصرية والكراهية.

* لا تستخدم لغة بذيئة وكلمات مبتذلة غير مقبولة اجتماعياً.

* لا تضع مشاركة سيئة بهدف حذفك لها لاحقاً فهنالك بعض التطبيقات تحفظ هذه المشاركات حتى بعد حذفك لها.

* عدم السماح والخوض في المحادثات الإباحية مع الأغراب أو الأصدقاء وتبادل الرسائل والصور والفيديوهات الخاصة المخلة للآداب والتي غالباً ما تفضي إلى الابتزاز.

* أخذ الحذر عند المشاركة في المجموعات والتي تحتوي على عدد كبير من الأشخاص فهي تزيد من احتمالية انتشار المحتوى بشكل سريع ضمن نطاق واسع والتعرض للمساءلة (مثل: تصوير شخص ما لغرض الاستهزاء به ونشر الفيديو ضمن المجموعات).



الآثار المترتبة من الاستخدام السلبي

يمكن أن يؤثر علينا التواجد في الفضاء السيبراني بشكل سلبي إن تم ادمان استخدام برامج التواصل الاجتماعي والألعاب الإلكترونية ومشاركة المعلومات الشخصية والعملية بشكل غير محدود و بلا وعي، ومن الآثار المحتملة ما يلي:

01 الميول للعزلة الاجتماعية

02 قلة النشاط البدني

03 الكسل والإرهاق

04 الصداع

05 الضغوط النفسية

06 اضطرابات النوم

07 زيادة الوزن

08 آلام جسدية بسبب وضعية الجلوس الخاطئة

09 مشاكل في العينين كالجفاف والشعور بالحرقان وزغلله النظر

10 التعرض لمحاولة الاحتيال





الهدف من النشاط هو تأكيد وصول المعلومة الصحيحة للمتدربين وتعزيز الإدراك للمفاهيم الأساسية.

سيتم إعطاء المتدربين فرصة لكتابة مشكلة قد حدثت لهم عند استخدام برامج التواصل الاجتماعي أو غيرها من الوسائل ضمن ساحة الفضاء السيبراني ومن دون كتابة اسماء أو أي معلومات شخصية عن المشاركين.

رابط الجرة الإلكترونية:

https://fs7.formsite.com/alibaro/lhvckzckdj/index.html





يجب على المتدربين وصف المشكلة وأثرها عليهم دون التطرق والحديث عما تم اتخاذه من إجراءات لحل المشكلة ويمكن الاكتفاء بذكر قد انتهت بالحل أوتم إهمالها دون حل.

بعد ذلك يقوم المدرب بجمع المدونات ضمن الجرة الإلكترونية.



يقوم المدرب بفتح بعض المدونات وليس جميعها وقراءتها وبدء النقاش لمعرفة الحلول المناسبة. كما سيتم نقاش المدونات والرد على البريد الالكتروني حال وجود استفسارات.



الجلسة الرابعة

ماهي أخطار الفضاء السيبراني؟

تتمحور أخطار الفضاء السيبراني في عدد من الأساليب الشهيرة للاختراق وانتهاك الخصوصية، ومنها:



الإصطياد الإلكتروني
عبارة عن مواقع او رسائل بريد إلكتروني من منتحل صممها مطابقة للأصلية تم تزويرها لغرض الاحتيال

الهندسة الإجتماعية
التحايل على المستخدم بغرض الحصول علي معلومات المفترض ألا يفصح عنها

ملفات طروادة
ملف يصلك ويبدو طبيعيا بينما هو عبارة عن برنامج خبيث



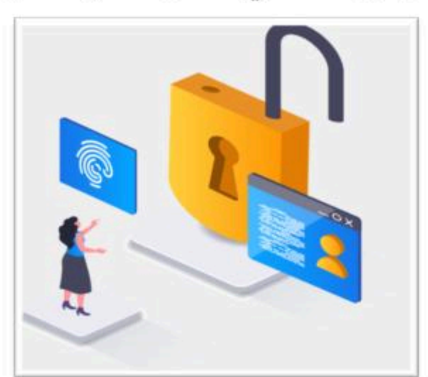
انتحال الشخصية
إنتحال شخصية أحد المشاهير أو الأقارب للحصول على معلومات من المفترض ألا تقوم بالافصاح عنها

الإبتزاز الإلكتروني
الحصول على معلومات أو مادة أو صورة إما انت طوعا بالاحتياط أو عن طريق الهجوم على جهاز الضحية ثم استخدامها ضده مقابل الحصول على المال



حماية الخصوصية في الفضاء السيبراني

يعرف موقع ويكيبيديا أن الخصوصية في الإنترنت "هي القدرة على تحديد المعلومات التي يكشفها الفرد عن نفسه أو يتحفظ عليها في الإنترنت وتحديد من الذي يمكنه الوصول إليها، ولأي أغراض يمكن أن تستخدم أو الأغراض التي لا يمكن أن تستخدم لها"، ومن هنا يجب علينا حفظ خصوصياتنا لكيلا يتم استغلالها واستخدامها بشكل سيء ومؤذي لنا.

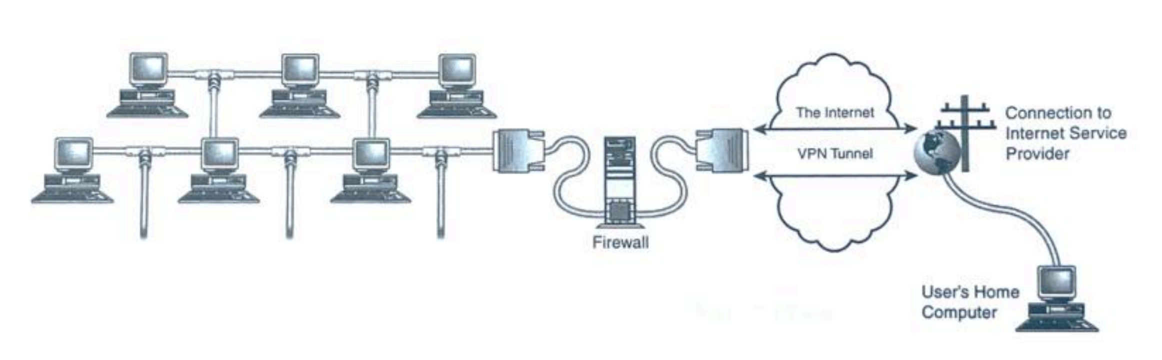


وفيما يلي عدد من النصائح لحفظ الخصوصية بالفضاء السيبراني:

- أن يتم استخدام كلمات المرور عند الدخول على أجهزتنا وجوالاتنا وحساباتنا في برامج التواصل الاجتماعي المختلفة.
- أن يتم استخدام كلمات مرور طويلة وقوية (أكثر من كلمة) وحفظها بشكل آمن وعدم الإفصاح عنها أو مشاركتها مع أي أحد حفاظاً على سريتها.
- تجنب استخدام كلمة مرور واحدة أو متكررة لعدة تطبيقات فإن تمت سرقة كلمة المرور استطاع المخترق سرقة الحسابات الأخرى.
- تجنب استخدام كلمات مرور يسهل تخمينها مثل الأسماء الشائعة، عيد ميلادك، رقم جوالك، اسمك الأول أو اسمك الأخير أو الكلمات والأرقام المتسلسلة: ABCD أو QWERTY أو 12345، كما يمكن أن يتم استخدام طرق بديلة مثل استخدام بصمة إصبع اليد أو بصمة العين / الوجه لمزيد من الحماية حال توفر ذلك.



- عدم تدوين كلمات المرور على الأوراق الصغيرة أو خلف البطاقات أو تحت لوحة المفاتيح او على ركن الشاشة أو ضمن سجل أرقام التواصل بالهاتف.
- احذر من متصفحي الأكتاف فهم يتربصون أي فرصة لمشاهدة كتابتك على لوحة المفاتيح وسرقة كلمات المرور.
- أن يتم تأمين البريد الإلكتروني والتطبيقات ببريد إلكتروني وأرقام هواتف استرجاع خاصة وآمنة كما يجب حماية التطبيقات المختلفة بمعايير التحقق الثنائي للوصول (الدخول بخطوتين) والتأكد من إعداد التشفير للبيانات حال توفرها.
- أن يتم إعداد الخصوصية ضمن برامج التواصل الاجتماعية وعدم إظهار المعلومات الشخصية للعموم وكذلك إظهار المشاركات للكل دون تحديد الأصدقاء أو مجموعات الأصدقاء.
- أن تتم مراجعة الملف الشخصي ومراقبة قائمة الأصدقاء والمضافين ضمن فترات معينة وإتاحة ذلك للآباء والأمهات لمراجعة القوائم بأنفسهم والتأكد من عدم وجود أشخاص غرباء مجهولين الهوية.
- الكثير من الأجهزة الذكية تقوم بحفظ موقع الجهاز خصوصاً عند تواجد خدمات تحديد المواقع GPS فيجب أن يتم الإعداد والحد من هذه الخدمات وعدم السماح بمشاركة مواقعك مع الآخرين حتى لا يتمكن أي غريب أو مجهول معرفة أماكن تواجدك عند استخدام التطبيقات المختلفة ومنع التربص.
- عدم استخدام شبكات الواي-فاي اللاسلكية العامة والمفتوحة فهي بيئة شبكية غير آمنة وقد يتم اختراق جهازك وسرقة بياناتك ومعلوماتك وحساباتك وانتهاك خصوصيتك مجرد قبول الانضمام بها.
- عدم مشاركة شبكات الواي-فاي اللاسلكية الخاصة بك او العائلية بالمنزل فبمجرد دخول الغرباء إليها قد يستطيعون اختراق كافة الأجهزة المتواجدة بالشبكة وسرقة المعلومات وفقدان الحسابات وانتهاك الخصوصيات.
- عند استخدام الشبكات الافتراضية VPN يجب التأكد من إعدادات الأمان مع مختصي تقنية المعلومات لاستكمال إعدادات الحماية والتشفير والجدار الناري وتوثيق أمن الوصول لشبكات العمل الرسمية.





إدراك حالات الخداع والتحايل السيبراني

لعل من أحد العوامل المؤثرة على أمن المعلومات في الساحة السيبرانية هو التعامل بحسن النية مع المخترقين والمخادعين حتى تقع الضحية في فخ الاحتيال ومشاركة المعتدين البيانات والمعلومات الحساسة وبذلك تتم سرقة الحسابات وانتهاك الخصوصية وقد تصل إلى سرقة الأموال.

من هنا يجب أن نحرص على ما يلي:

- عند تواجدك في الفضاء السيبراني فتوقع دائماً أن هناك من يراقبك ويحاول خداعك وسرقتك.

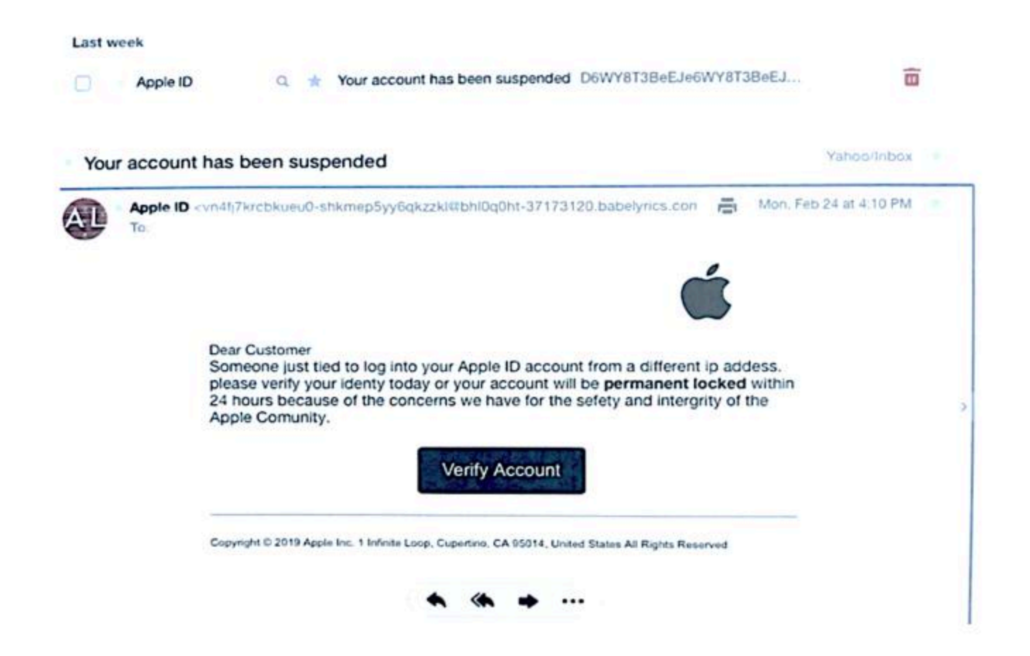


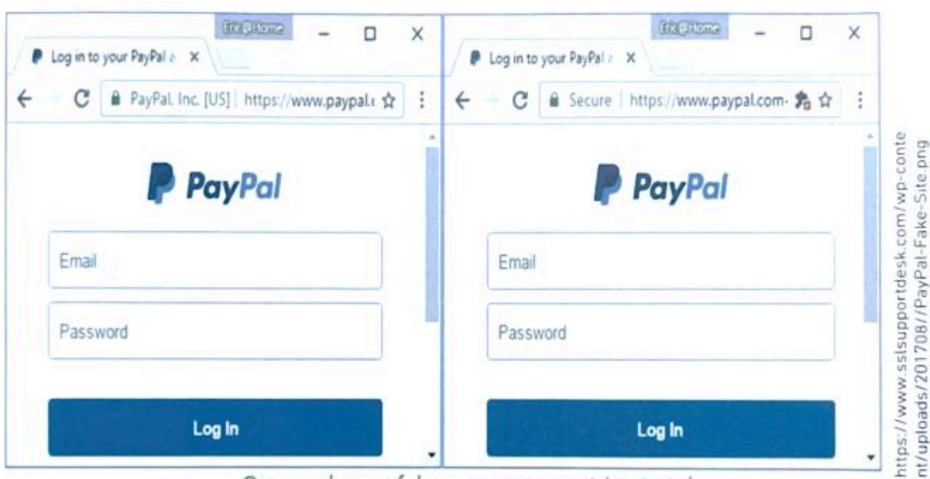
- لربما يستغل المعتدين تواجد معلوماتنا الشخصية المتاحة للجميع ضمن برامج التواصل الاجتماعي فيقومون بجمعها وقد يستغلون بعض الأصدقاء لجمع بيانات أكثر منهم عننا وبعدها تبدأ لعبة الاحتيال والحديث معنا وكأنهم أصدقاء وإبداء المساعدة لنا وهم في الحقيقة مخادعين غرضهم الخداع وسرقة البيانات والمعلومات الحساسة منا.
- قد يستغل المعتدي خداعك من خلال جهاز أو حساب صديقك المخترق ويبدأ الحديث معك وكأنه صديقك فعلاً وتبدأ المطالبة بمشاركة المعلومات الحساسة أو طلب المساعدة المالية أو غيرها. هنا يجب أن يتم التأكد من هويته المتحدث والاتصال المباشر بصديقك أو مقابلته وجهاً لوجه خصوصاً في القضايا الهامة.
- وقد يستغل بعض المعتدين حجة الفوز بالجوائز والمسابقات الوهمية وماهي إلا وسيلة أخرى للتحايل وسلب الضحايا معلوماتهم الهامة والشخصية الخاصة للوقوع في فخ يكلفهم الكثير من الخسائر بدلاً من الفوز والربح.





- التزييف والخداع أحد أخطر وسائل الهجوم واصطياد الضحايا، والصور أدناه توضح بعض تلك الطرق، في الصورة الأولى بريد إلكتروني بصيغة رسمية وهوية شركة موثوق بها ولكن من عنوان بريدي مزيف، والثانية توضح تصميم لصفحة شركة باي بال المعروفة ولكن من عنوان رابط مزيف.





One real, one fake, your account is at stake.

أولاً ماذا نعني بالهندسة الاجتماعية؟

الهندسة الاجتماعية (Social Engineering) تعرف بفن التلاعب وخداع المستخدمين حتى يصرحوا ببياناتهم ومعلوماتهم السرية والخاصة لاستغلالها في أغراض الاختراق وسرقة الحسابات وانتهاك الخصوصية وانتحال الشخصية وسرقة الأموال وغيرها من الجرائم المعلوماتية.

يقوم المعتدي باستخدام الذكاء الاجتماعي والصوت البريء وإظهار حسن النية واستعداده في تقديم المساعدة والعون وإيهام الناس بأن التعامل معه سيفيدهم وذلك بتحقيق مصالح لهم مثل تحديث النظام وتطوير الأدوات التقنية وتسريع الخدمات والإنترنت وإصلاح الأعطال وغيرها من الادعاءات ويقوم المعتدي بطلب بعض البيانات السرية بحجة التأكد من هويتهم وأنها متطلبة من مقدم الخدمة ويقوم بطلب بيانات دخول المستخدم على النظام أو التطبيق وكلمات المرور وأرقام هاتف الجوال وأرقام الهوية الوطنية أو الجواز أو الحسابات البنكية وأرقام البطاقات الائتمانية وغيرها من البيانات الحساسة والتي لا يجب مشاركتها مع أي أحد حفاظاً على سريتها.



النشاط الثالث:

يظهر أحد سـيناريوهات الهندسـة الاجتماعية وهي بين أحد الطلبة المسـتخدمين لنظام أو منصـة التعليم الإلكتروني المعتمدة من وزارة التعليم وأحد محترفي التصيد الإلكتروني، وقد تعرض الطالب للخداع باستخدام الهندسة الاجتماعية.

محور النقاش: ما هو التصرف الأمثل عند مواجهة هذا الفخ السيبراني؟

https://fs7.formsite.com/alibaro/jnuhpeop4n/index.html?1628589658724



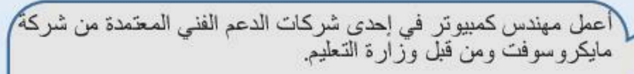
ملاحظة: السيناريو يعتبر تخيلي مبنى على الخبرات وبعض القصص المشابهة.

عملية الاحتيال تتم عبر إحدى برامج التواصل الاجتماعي مثل واتس أب أو تليغرام أو غيرها



الضحية

معتدي: مرحباً.. أنا اسمي نعيم



معتدي: أعمل مهندس كمبيوتر في إحدى شركات الدعم الفني المعتمدة من شركة مايكروسوفت ومن قبل وزارة التعليم.

أتواصل معك اليوم بسبب ظهور رسالة من جهازك تطلب تحديث النظام وعمل صيانة دورية لزيادة سرعة الانترنت ومن بعدها سرعة الدخول على نظام الوزارة وحضور كافة الفصول الافتراضية بسهولة .

الضحية: أهلا وسهلا !! شكراً أخ نعيم

الضحية: صحيح فأنا أعاني منذ فترة من عدم سرعة الانترنت وتعليق الجهاز المتكرر في المنصة واحتاج منك أن تخدمني وتحدث جهازي وتنزل كافة الأدوات المجانية لكي أتمكن من استخدام النظام والمنصة بكل يسر وسهولة .

معتدي: نسعد بخدمتكم واحتاج منك بعض البيانات البسيطة لإتمام عملية التحديث والتي تطلبها الوزارة لعمل الإحصاءات وإثبات تقديم الخدمات لكم.

فضلاً إرسال اسم المستخدم وكلمة المرور / إيميلك الشخصي وإيميل ولي الأمر / رقم الجوال ورقم جوال ولي الأمر /يفضل أن تعطيني كذلك أرقام الهوية الوطنية لإثبات حضوركم بالفصول الافتراضية .

الضحية:
اسم المستخدم على المنصة Ahmad
كلمة المرور : AhMadA20

جوال : 05500000000
جوال ولي الأمر : 0500000000

الهوية : 012012012012
الإيميل : asdggg@gmail.com
إيميل والدي : assdjh@gmail.com

معتدي: آخر شيء هناك بعض الخدمات التي وفرتها الوزارة لكم مجاناً وتم دفع قيمتها، ولكن لكي يتم انزالها لكم بالجهاز نحتاج إلى ما يثبت موافقة ولي الأمر والأمر بسيط هو فقط إدخل رقم البطاقة الائتمانية وتاريخها ورقم التحقق وهي فقط لإثبات الموافقة ولن يتم سحب أي مبلغ منها فالخدمات قد دفعتها لكم الوزارة بالكامل مشكورة على ذلك...

الضحية:
رقم بطاقة الفيزا :
2136-9784-6548-6543
اسم صاحب البطاقة : Masud A.
تاريخها : 08/22
رقم التحقق خلف البطاقة : 156

الضحية: شكراً لكم وأتمنى أن تعطيني خبر أو ما تنتهي وتصلح النظام ..

وألف شكر لكم .

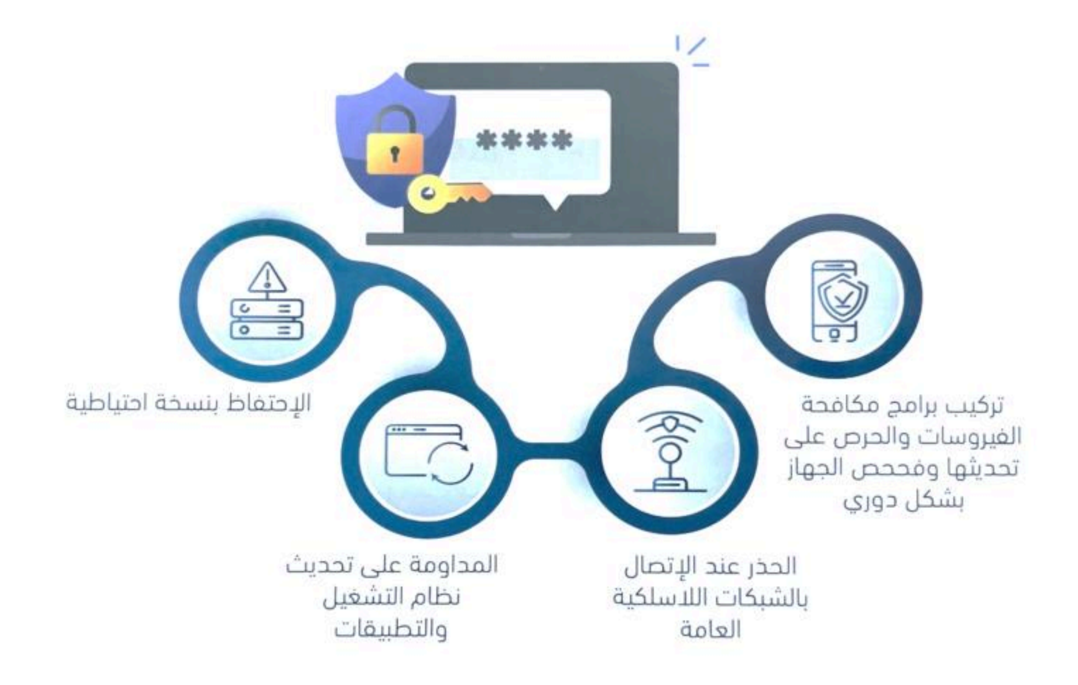
معتدي: بكل سرور وسنعمل جاهدين لخدمتكم ...



الجلسة الخامسة

ماهي أهم الإرشادات التي يوصي بها المختصين؟

لعله من أهم الأمور هو المحافظة على أمن جهازك وملفاتك والمداومة على ما يلي:



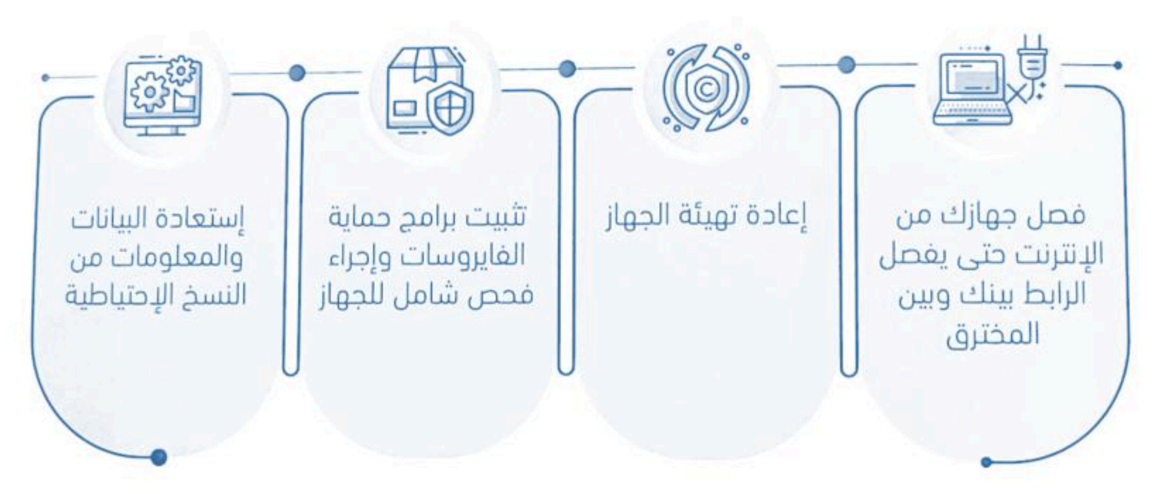
حسناً، ماذا أفعل عندما أتعرض لأي اعتداء إلكتروني؟

- يجب عليك في البداية تجاهل الرسائل من المعتدين والغرباء وحظر الأرقام والحسابات المجهولة.
- يجب التوقف عن مشاركة المعتدي أو المهاجم أو الغرباء بشكل عام أي معلومات خاصة.
- يجب عليك عدم الرد على المعتدي والاعتداء عليه بالمثل فهو سلوك خاطئ قد يضعك في خانة الاتهام ويفقدك حقك في المطالبة بالدفاع.
- كما يجب عدم السكوت عن الاعتداء ويجب أن يتم الإبلاغ عنه وعدم التجاهل في حال استمرار المعتدي بالمضايقة والتهديد لكيلا تكبر المشكلة وتزيد من أثارها السلبية عليك.
- عدم الحرج من نقاش أي حالة اعتداء عليك مع المقربين أو الأصدقاء الثقات، وإن كانت معلومات تخص العمل فيجب إبلاغ المسؤولين في العمل مثل الرئيس المباشر أو من تثقون به كمختص تقنية المعلومات.

- البدء في جمع وحفظ كافة الرسائل المتبادلة كدليل وشاهد يثبت حالة الاختراق أو الاعتداء ونوعه وعدم حذف الأدلة وإن طلب المعتدي ذلك.
- يمكن الدخول على تطبيق "كلنا أمن" واختيار الجرائم المعلوماتية في حال تم تصنيف الاعتداء كجريمة إلكترونية أو معلوماتية.
- يكون رفع بلاغ الجرائم الإلكترونية من خلال التطبيق كلنا أمن ويجب اختيار نوع البلاغ من أحد الخيارات المتاحة بالتطبيق وهي:
  - ذكر نوع التطبيق الذي تم حدوث الاعتداء من خلاله: تويتر، انستقرام، سناب شات، يوتيوب، فيسبوك، أو غيره.
  - كتابة حساب المعتدي مع رابط الحدث ضمن البلاغ وذكر حالة الحساب: هل هو نشط او غير نشط أو محذوف.
  - شرح وافي عن حالة الاعتداء وارفاق المستندات المساندة والداعمة التي تثبت الحالة.
- الانتظار بعد إرسال البلاغ والتأكد من استلام الرقم المرجعي للبلاغ لبدء الجهات المختصة في التحري واتخاذ ما يلزم نظاماً.
- عدم إبلاغ المعتدي بأنه قد تم رفع بلاغ عنه، كما لا يجب التواصل معه شخصياً عبر أرقام هواتف أو البريد الإلكتروني أو حسابات أخرى.
- يفضل عدم قبول أي إضافات لصداقات مجهولة وذلك لإغلاق فرصة تواصل المعتدي مرة أخرى بعد حظره من خلال حسابات جديدة.
- الإبقاء قريباً مع المختصين ومنحهم فرصة مراقبة الحساب الشخصي لفترة حتى يتم التأكد من سلامة الاستخدام وزوال الخطر.
- العودة إلى استخدام التطبيقات يجب أن يكون بحذر وبشكل آمن بعد معرفة وإدراك كافة المخاطر المحتملة وكيفية منعها والتصدي لها.
- في حال حصول الاعتداء على أحد من أصدقائك أو الأقرباء فلا تتردد بالإبلاغ وإتباع الخطوات السليمة ومساعدتهم، ومساندتهم، ونصحهم، وإرشادهم.

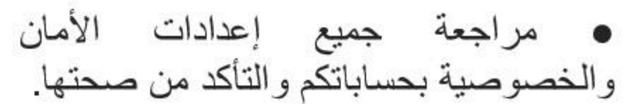


ومن الخطوات التقنية الهامة لاستعادة السيطرة بعد اختراق الجهاز:



وفي حال اختراق أحد الحسابات الخاصة بكم فيجب إتباع النصائح التالية:

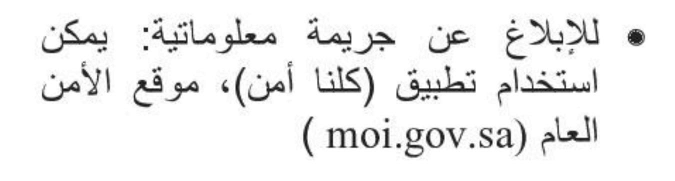
- تغيير كلمة المرور الخاص بالحساب الذي تم اختراقه على الفور وبكلمة جديدة
- البحث عن أي تحديثات جديدة للأنظمة والأجهزة والتطبيقات لضمان سد أي ثغرة أمنية قد يمكن استغلالها.
- مراجعة جميع إعدادات الأمان والخصوصية بحساباتكم والتأكد من صحتها.



- الإبلاغ عن الاختراق وتحذير جميع من قد يتمكن المخترق من التواصل معهم منتحلاً شخصية صاحب الحساب المخترق.
- التواصل مع إدارة الحساب أو الشركة أو مسؤول تقنية المعلومات والابلاغ عن الاختراق لكي يتمكنوا من فحص الاختراق ومعرفة ما إذا كان هناك ثغرات جديدة قد يمكن استغلالها.
- عدم الاستجابة لأي طلبات جديدة من أي مجهول وتفادي فتح وتتبع الروابط الغير آمنه والمجهولة المصدر.

كما هنالك الكثير من الجهات المعتبرة والتي تمنح فرصة التواصل المباشر وأخذ المشورة وإرسال الاستفسارات وأخذ الإجابات الموثوقة للمساعدة والدعم والإرشاد، وقد وفرت لنا حكومتنا الرشيدة العديد من المؤسسات التنظيمية والخدمات الإلكترونية لحفظ حقوق المواطنين بشكل عام وذلك لإرشادهم وخدمتهم وحمايتهم. فيجب الحرص على معرفتها والاستفادة منها، من المصادر ما يلي:





- للإبلاغ عن جريمة معلوماتية: يمكن استخدام تطبيق (كلنا أمن)، موقع الأمن العام (moi.gov.sa)



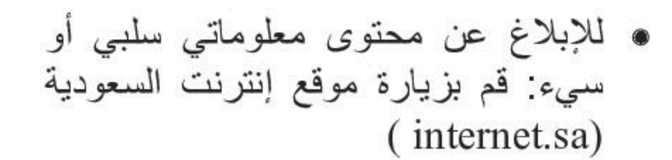


- عند وجود أسئلة عن أمن المعلومات: قم بزيارة موقع المركز الوطني الإرشادي للأمن السيبراني (cert.gov.sa)



- للإبلاغ عن مشاكل في خدمات الاتصالات: قم بزيارة موقع هيئة الاتصالات وتقنية المعلومات (www.citc.gov.sa)





- للإبلاغ عن محتوى معلوماتي سلبي أو سيء: قم بزيارة موقع إنترنت السعودية (internet.sa)



- للإبلاغ عن محتوى مخل للآداب: قم بزيارة موقع اللجنة الوطنية لتقنين المحتوى الأخلاقي لتقنية المعلومات (ncdcr.gov.sa)



وعند الحاجة الى الاستشارات النفسية الفورية يمكنكم التواصل مع الجهات التالية:



بالتواصل مع مركز اتصال الاستشارات النفسية على الرقم (920033360) من الأحد إلى الخميس من 8 صباحاً - 4 عصراً



طلب الاستشارة نصياً أو عبر تسجيل صوتي في أي وقت من خلال تطبيق قريبون (التطبيق متاح في متجر أبل وقوقل بلاي)



التواصل مع خط مساندة الطفل على الرقم (116111) للاستشارات الفورية أو التبليغ عن الاساءات التي تحدث للأطفال

ملاحظة:
جميع الاستشارات تقدم من قبل مختصين في الجانب النفسي والاجتماعي وبسرية تامة.



نشاط مقياس الممارسات الإلكترونية الخاطئة



يهدف هذا النشاط إلى توعية المتدربين بالمفاهيم الأساسية بالأمن السيبراني ويمكنهم من قياس مدى التقبل أو الرفض لكثير من الممارسات التي تصنف بأنها استخدامات خاطئة:

يعتبر نشاط فردي حيث يقوم المتدرب بالإجابة على كل عبارة إما بالموافقة أو عدم الموافقة ولكافة العبارات.



بعد ذلك يقوم المدرب بنقاش نتائج المقياس مع المتدربين ومعرفة فيما إذا كان هنالك تقبل أو رفض أو حياد للممارسات الخاطئة.

المقياس متوفر عبر الإنترنت وإمكانية القياس إلكترونياً من خلال الرابط أدناه:

https://fs7.formsite.com/alibaro/8emcyeozi2/index.html





كشف نتيجـــة حساب المقياس



معادلة حساب النتيجة

(عدد عبارات نعم ✖ 4) ➕ (عدد عبارات لا ✖ 2)

ضع/ ضعي نتيجتك هنا



44-32
تعني الرفض



50-46
تعني الحياد

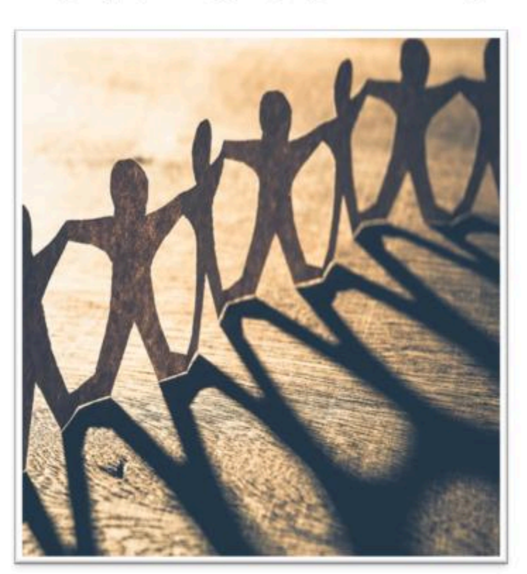


64-52
تعني القبول

من أهمية التطور التكنولوجي في حياتنا أصبح واجب علينا أن نحافظ على معلوماتنا في البيئة السيبرانية لضمان بقائها واستمرارها، ومن هنا نقدم أهم عشر نصائح مستله من كتاب الوصايا العشر في الأمن السيبراني (المبيض، ٢٠٢٠):

* الوصـايـا العشـر في الأمن السيبرانـــي *	
أولاً: مستوى أمان كلمة المرور يجب التأكد على أن تكون كلمات المرور الخاصة بكم صعبةً وغيرَ منطقية ويفضل أن تحمل حروف وأرقام ورمز خاص بكم إن أمكن، كلما كانت كلمة المرور صعبه وغير متوقعه كلما كان من الصعب تفكيك الشفرة الخاصة.	
ثانياً: كلمة مرور مختلفة لكل حساب فلا يجب استخدام كلمة مرور واحدة لجميع حساباتكم الإلكترونية، من لديه كلمة مرور واحده لكل حساباته فهو كمن ينطبق عليه المثل (من يضع البيض في سلة واحدة) فعلى الأقل يجب أن تكون لديك ثلاث أو أربع كلمات مرور قوية.	
ثالثاً: التحقق بخطوتين لضمان سلامة حساباتكم من الاختراق ولضمان أيضاً استعادتها بعد فقدان أو نسيان الأرقام السرية يحب عليكم بتفعيل خطوات التحقق الثنائي أو التحقق من خطوتين، التحقق الثنائي هو التحقق عن هُوية المستخدم من مصدرين مختلفين لضمان اثبات هُوية صاحب الحساب الفعلي.	
رابعاً: برامج الحماية المعلوماتية يجب ألا تتهاونوا في اقتناء برامج الحماية الموثوقة وتحديثها بشكل دوري، ويتوجب عليكم بتحديث برامج الحماية الموجودة على جميع أجهزتكم حتى تكون بياناتكم وملفاتكم وشبكاتكم بأمان من جميع البرامج والملفات الضارة.	
خامساً: البرامج ذاتُ المصادر غير المعروفة يجب أن لا تقوموا بفتح أو تحميل البرامج ذات المصادر المجهولة أو غير الموثوقة، وذلك لضمان سلامتها وخلوها من أي ملفات ضارة تسمح للمخترقين من خلالها الوصول إلى بياناتكم وأجهزتكم الخاصة.	
سادساً: تقليد البرامج والرسائل الإلكترونية احذروا التقليد ❗ هذه العبارة تُكتب دائماً على الكثير من المنتجات الاستهلاكية العينية، وذلك لتحذير المستهلكين من وجود بضائع مطابقة للمنتج. أما في عالم التكنولوجيا فيعتبر التقليد هو من أكثر الاختراقات شيوعاً ومن أكثرها حصداً للضحايا.	
سابعاً: شبكات WI-FI للأسف هي شبكات انترنت عامة تشكل خطراً شديداً على سلامة أجهزتكم وبياناتكم والاشتراك مع الأشخاص المجهولين بشبكة واحده يشكل ثغرة أمنية سهلةً للمخترقين ومما يتيح لهم سرقة العديد من البيانات المسجلة على أجهزتكم ويجب علينا عدم مشاركة أجهزتنا بشبكات عامة.	
ثامناً: النسخ الاحتياطي من الجيد عمل نسخ احتياطي لبياناتكم بشكل دوري، وذلك لسهولة حفظها والعودة لها في حال تم فقدانها من أجهزتكم بسبب خلل تقني أو أمني.. ويفضل أن يكون النسخ الاحتياطي لبياناتكم أن يكون مجاني غير مدفوع وذلك لضمان استمرارية النسخة الاحتياطية للبيانات.	
تاسعاً: تحديث البرامج والأنظمة والتطبيقات يجب أن يكون بشكل دوري وفي حال صدور تحديثات لأي منها للحماية المثلى، كما أن تحديث أنظمة أجهزتكم وتطبيقاتكم يتيح للشركات والمطورين من تطوير وسائل الحماية وسد الثغرات الأمنية المُكتشَفة.	
عاشراً: بياناتكم الشخصية المخترقون بالعادة يجمعون معلومات ضحاياهم لتحليلها وتحديد طريقة الاختراق المناسبة ونقاط الضعف والثغرات المتاحة في المواقع التواصل الاجتماعي، لذلك عليكم التقليل من نشر معلوماتكم عبر الإنترنت، فهو يعتبر أمر صحي لأمن معلوماتكم وخصوصياتكم.	

وفي الختام، فيجب أن يكون كل فرد واعي بأهمية الحماية والملكية والخصوصية في الفضاء السيبراني وحماية المعلومات الشخصية والمعلومات المتعلقة بأسرته وأصدقائه وعمله ومنظمته ووطنه وعدم المشاركة الا لمن يستحق بعد التحقق من المعلومات التي يمكن المشاركة بها فكما ليس كل ماء صالح للشرب فليست كل معلومة صالحة للمشاركة. ولنعلم جيداً أن بعد الضغط على إزرار إرسال أصبحت المعلومة ملك المستلم وحتى بعد حذفها من جهازك ويظهر لك البرنامج مسحها فهي في مكان ما بداخل خوادم الشركة المقدمة للخدمة ولها الحق في مشاهدتها وتحليلها ومشاركتها وبيعها في بعض الاحوال، فأحرص أن معلوماتك الشخصية وصورك الجميلة ليست للعرض والتداول وأن كان البعض يقول الجملة الشهيرة "هل أنا من بين كل الملايين سيتم اخذ صوري" ولما لا يكون استخدام الذكاء الاصطناعي له دور في ذلك بعدد المشاهدات او عدد الاعجاب او المشاركات بالمنطقة وغيرها من المحددات ويتم الاختيار بناء على ذلك. نسبة حدوث ذلك قد تكون ضئيلة، ولكن لا يمكن ان نقول مستحيلة، فالفضاء السيبراني في اتساع دائم وإن لم نحرص فقد نندم وهنالك تطور مستمر في وسائل وأساليب الهندسة الاجتماعية والتي زادت من حالات السرقات والتحايل وانتحال الشخصيات والابتزاز وغيرها من الجرائم المعلوماتية، وتقع مسؤولية نشر الوعي والامن على الجميع وتبدأ من المنزل بين الأبناء والاباء والامهات والعائلة بين الأشقاء والأقرباء الى الموظف والمسؤول في الأعمال والمعلم والمعلمة في المدارس والجامعات وحتى بين الأصدقاء وحتى بين افراد المجتمع من قد نتواصل معهم في الفضاء السيبراني المتسع.



كسر شفرت (Enigma) في الحرب العالمية كان بسبب التهاون لإجراءات الاستخدام الصحيح

فلا تتهاونوا عند الاستخدام والمشاركة حفظكم الله ...

Workshop evaluation - استبانة تقييم ورشة العمل

Full Name - الإسم الكامل

eMail - البريد الإلكتروني

Choose the best answer for each of the following - اختر افضل اختيار لما يلي *

	Strongly Agree - اتفق بشدة	Agree - اتفق	Neutral - محايد	Disagree - لا اتفق	Strongly Disagree - لا اتفق بشدة
The presenter(s) communicated clearly - كان تواصل المدرب واضح	○	○	○	○	○
I learned something new - قد تعلمت شيئاً جديداً	○	○	○	○	○
This course was relevant to my position - المعلومات كانت مناسبة لي	○	○	○	○	○
This course was a valuable use of my time - كان البرنامج مفيداً واستغل وقتي جيداً	○	○	○	○	○
The level of recived knowledge was enough - كمية المعلومات المستلمة كانت كافية	○	○	○	○	○

How difficult was this course for the amount of material it covered? - لأي مدى كان محتوى المادة العلمية صعباً *

○ Too Difficult - صعب جدا ○ Difficult - صعب ○ Average - متوسط ○ Easy - سهل ○ Too Easy - سهل جدا

How long was this course for the amount of material it covered? لاي مدى كان طول المدة المطلوبة لانهاء البرنامج *

○ Too long - طويلة جدا ○ Long - طويلة ○ Average - متوسطة ○ Short - قصيرة ○ Too short - قصيرة جدا

Overall, how satisfied were you with this training course? بشكل عام، ماهو مدى رضاكم عن البرنامج *

○ Very Satisfied - راضي جدا ○ Satisfied - راضي ○ Neutral - محايد ○ Dissatisfied - غير راضي ○ Very Dissatisfied - غير راضي جدا

How likely would you be to recommend this course to a coworker or colleague? لاي مدى تنصح الموظفين اخذ هذا البرنامج التدريبي *

○ Very Likely - محتمل جدا ○ Likely - محتمل ○ Neutral - محايد ○ Unlikely - مستبعد ○ Very Unlikely - مستبعد جدا

Comments or Suggestions - هل لديكم أي ملاحظات تحسينية للمستقبل

تتوفر الاستبانة عبر الرابط التالي: https://fs7.formsite.com/alibaro/kc4eiwlfyy/index.html

استبانة التقييم البعدي لقياس وعي المتدربين بمفاهيم الأمن السيبراني.

أرجوا قراءة العبارات التالية والإجابة بـ (نعم) حال الموافقة على ما تم ذكره بالعبارة والاجابة بـ (لا) حال عدم الموافقة عليها:

العبـــــــــــــــــارة	نعم	لا
أقوم باستخدام برمجيات وتطبيقات خاصة لحماية جهازي من الاختراق والتجسس والفيروسات		
احتفظ بالبيانات الخاصة بي في أكثر من مكان لتفادي فقدانها او تلفها		
أقوم بنسخ البيانات الخاصة بي احتياطياً في ذاكرة خارجية وحفظها بمكان آمن		
اسمح بمشاركة معلوماتي الشخصية للأصدقاء عبر الإنترنت وبرامج التواصل الاجتماعي وغيرها من الوسائل بالفضاء السيبراني		
اسمح بمشاركة معلوماتي الشخصية للغرباء عبر الإنترنت وبرامج التواصل الاجتماعي وغيرها من الوسائل بالفضاء السيبراني		
اسمح بمشاركة بعض معلوماتي الشخصية غير الحساسة للأصدقاء عبر الإنترنت وبرامج التواصل الاجتماعي وغيرها من الوسائل بالفضاء السيبراني		
اسمح بمشاركة بعض معلوماتي الشخصية غير الحساسة للغرباء عبر الإنترنت وبرامج التواصل الاجتماعي وغيرها من الوسائل بالفضاء السيبراني		
احرص على تجنب مشاركة المعلومات المخالفة للعقيدة، او الدين، او القوانين، او الأعراف، او التقاليد		
دائما ما اراعي أراء الآخرين ومشاعرهم عند مناقشة موضوع ما عبر الإنترنت		
أصبح لدي وعي كافي بأنظمة المملكة العربية السعودية المتعلقة بالأمن السيبراني يمكنني من التعامل مع الإنترنت وبرامج التواصل الاجتماعي بشكل آمن وصحيح		
أشدد على ضرورة توعية المستخدمين/ الموظفين/ الطلبة بمفاهيم الامن السيبراني والتعليمات والقوانين والمخالفات والعقوبات المتعلقة بلستخدام الإنترنت وبرامج التواصل الاجتماعي		
أؤيد وضع إجراءات وسياسات واضحة لحفظ الأمن السيبراني الخاصة بمشاركة المعلومات ونقلها عبر الإنترنت		



قائمـة المراجـع العربيـة:

1. الحربي، شيخة عمران ابراهيم. (2019). العوامل الاجتماعية المرتبطة بالجرائم السيبرانية: دراسة ميدانية. رسالة (ماجستير)-جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاجتماعية، قسم علم الاجتماع، تخصص تأهيل ورعاية اجتماعية. رابط:

https://repository.nauss.edu.sa/handle/123456789/66248

2. بن عباس, ناصر بن محمد ناصر. (2020). تدابير وقائية مقترحة للوقاية من الجرائم السيبرانية: دراسة ميدانية. أطروحة (دكتوراه)-جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاجتماعية، قسم علم الاجتماع، تخصص علم اجتماع الجريمة. رابط:

https://repository.nauss.edu.sa/handle/123456789/66908

3. نظام مكافحة جرائم المعلوماتية. (2007). هيئة الاتصالات وتقنية المعلومات. ص.(1-5).الرابط:

https://www.citc.gov.sa/ar/RulesandSystems/CITCSystem/Documents/LA_004_%20A_%20Anti-Cyber%20Crime%20Law.pdf

4. المنتشري، فاطمة يوسف، حريري، رندة. (2020). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات . المجلة العربية للتربية النوعية. مج. 4، ع. 14، يوليو 2020. ص ص. 95-140). الرابط:

http://search.shamaa.org/FullRecord?ID=260482

5. المبيض، محمد شاكر. (٢٠٢٠). الوصايا العشر في الأمن السيبراني. الرياض، المملكة العربية السعودية، مطبعة الحميضي.

6. التنمر آفة لا نراها. (٢٠٢١). دليل الآباء الإرشادي للأطفال في العالم الرقمي. وزارة الاتصالات وتقنية المعلومات، المملكة العربية السعودية. ص. ١-ص.٣٤. يمكن الوصول عبر الرابط :

https://cyberbullying.attaa.sa/Parents-guide-for-children-in-the-digital-world-new.pdf

قائمـة المراجع الأجنبيـة:

1. Aiken, M. (2017). The cyber effect: A pioneering cyber-psychologist explains how human behavior changes online. London, United Kingdom, John Murray Press.
2. Albar, A. A., (2017). Aggression in Cyber Sphere: A Qualitative Study to Explore Saudi Arabian Social Media. Knowledge Discovery and Data Design Innovation, pp. 145-170. Retrieved from https://www.worldscientific.com/doi/abs/10.1142/9789813234482_0008
3. Albar, A. A., (2018). Development of Scales to Measure the Level of Aggression in Saudi Cyber Sphere. A conference paper presented in “The 21st Saudi Computer Society National Computer Conference (SCS-NCC’2018)”. Riyadh, Kingdom of Saudi Arabia. pp. 1-8. doi:10.1109/NCG.2018.8593167. Retrieved from https://ieeexplore.ieee.org/abstract/document/8593167/references#references
4. Al-Zahrani, A. M. (2015). Cyberbullying among Saudi’s higher-education students: Implications for educators and policymakers. *World Journal of Education, 5*(3), 15-26. Retrieved from https://files.eric.ed.gov/fulltext/EJ1158405.pdf
5. Starcevic, V., & Aboujaoude, E. (2015). Cyberchondria, cyberbullying, cybersuicide, cybersex: “new” psychopathologies for the 21st century? *World Psychiatry, 14*(1), 97-100.

الملحق (أ)

K ماذا أعرف؟	W ماذا أريد أن أعرف؟	L ماذا تعلمت؟

أسئلة لازالت لديّ (Q)؟

....

....

....

....

....



الملحق (ب)

بيانات التواصل المباشر مع باحث/ مؤلف/ معد/ مقدم الحقيبة التدريبية:

Royal Commission for Jubail & Yanbu  الهيئة الملكية للجبيل وينبع

د. علي بن عيدروس بن علي البار
وكيل وكالة التعليم الإلكتروني
وكالة التعليم الإلكتروني
قطاع التعليم – الهيئة الملكية بينبع

مدينة ينبع الصناعية – العزيزية - كلية ينبع الجامعية – مبنى E – مكتب E2-006

Dr. Ali A. Albar
Managing Director, eLearning Directorate
eLearning Directorate,
Division of Education - Royal Commission Yanbu

Yanbu Industrial City- Yanbu University College- Building (E) – Office (E2-006)

+966-50-552-2558  014-394-61000 (Ext. 1580)

 albara@rcyci.edu.sa  www.ali-albar.net

WWW.RCJY.GOV.SA

Note: According to the new security policies, I will not be able to receive emails from public email providers (i.e., @gmail, @yahoo, @hotmail, etc.)

